In the claims:

1. A method for encrypting electronic books, comprising:

supplying an electronic book to be encrypted;

supplying an encryption key;

encrypting the electronic book using the encryption key;

supplying the encrypted electronic book;

supplying a decryption key; and

decrypting the encrypted electronic book using the decryption key.

2. The method of claim 1, wherein the encryption key and the decryption key are a symmetric key.

3. The method of claim 2, further comprising generating the symmetric key.

4. The method of claim 3, wherein the symmetric key is generated randomly.

5. The method of claim 3, wherein the symmetric key is generated using a key generator.

6. The method of claim 2, further comprising retrieving the symmetric key from a key storage memory.

7. The method of claim 2, wherein the symmetric key is a transaction symmetric key, the transaction symmetric key supplied by a certificate authority.

8. The method of claim 7, further comprising:

sending a transaction symmetric key request to the certificate authority;

encrypting the transaction symmetric key using a first party symmetric key to produce a first encrypted transaction symmetric key;

delivering the first encrypted transaction symmetric key to a first party;

decrypting the first encrypted transaction symmetric key, wherein the electronic book is encrypted by the first party using the transaction symmetric key;

encrypting the transaction symmetric key using a second party symmetric key to produce a second encrypted transaction symmetric key;

delivering the second encrypted transaction symmetric key to a second party; and

decrypting the second encrypted transaction symmetric key, wherein the electronic book is decrypted using the transaction symmetric key.

9. The method of claim 2, wherein the electronic book content and a transaction symmetric key are encrypted by a first party and wherein the encrypted electronic book content is supplied to a second party and the encrypted transaction symmetric key is supplied to a third party.

10. The method of claim 9, wherein the second party requests the encrypted transaction symmetric key from the third party.

11. The method of claim 10, wherein the third party decrypts the encrypted transaction symmetric key using a first party symmetric key.

12. The method of claim 11, further comprising:

encrypting the decrypted transaction symmetric key using a second party symmetric key;

supplying the encrypted transaction key to the second party; and

decrypting the encrypted transaction symmetric key using the second party symmetric key.

13. The method of claim 12, further comprising completing a financial transaction between the first party and the second party before supplying the encrypted electronic book.

14. The method of claim 12, wherein the first party is an electronic book publisher, the second party is an operations center of an electronic book distribution system and the third party is a certificate authority.

15. The method of claim 12, wherein the first party is an electronic book distributor, the second party is an electronic book viewer and the third party is a certificate authority.

16. The method of claim 2, further comprising:

encrypting the symmetric key with a private key and a private key encryption process;

packaging the encrypted symmetric key and the encrypted electronic book; and

delivering the package to an electronic book viewer.

17. The method of claim 16, further comprising:

decrypting the encrypted symmetric key using a public key and a public key decryption process; and

decrypting the encrypted electronic book using the decrypted symmetric key.

18. The method of claim 17, wherein the encryption method is one of a Merkle-Hellman Knapsack technique, a RSA technique, a Pohlig-Hellman technique and a Schnorr Signature technique.

19. The method of claim 2, wherein the symmetric key is a transaction symmetric key, further comprising:

generating the transaction symmetric key at a first party location;

encrypting the electronic book using the transaction symmetric key and a symmetric key encryption process;

delivering the encrypted electronic book to a second party;

encrypting the transaction symmetric key using a first shared symmetric key and a first symmetric key encryption process;

delivering the encrypted transaction key to a third party;

decrypting the encrypted transaction symmetric key using the first shared symmetric key and a first symmetric key decryption process;

requesting the decrypted transaction symmetric key from the third party;

encrypting the transaction symmetric key using a second shared symmetric key and a second symmetric key encryption process;

delivering the encrypted transaction symmetric key to the third party;

decrypting the encrypted transaction symmetric key using the second shared symmetric key and a second symmetric key decryption process; and

decrypting the delivered electronic book using the decrypted transaction symmetric key.

20. The method of claim 19, further comprising completing a financial transaction between the first party and the second party prior to delivery of the encrypted electronic book.

21. The method of claim 19, further comprising completing a financial transaction between the first party and the second party prior to delivery of the encrypted transaction symmetric key to the second party.

22. The method of claim 2, wherein the symmetric key is a shared transaction symmetric key, further comprising negotiating the shared transaction symmetric key

between a first party and a second party, wherein the first party supplies the encrypted electronic book to the second party.

23. The method of claim 22, wherein the shared transaction symmetric key is generated by first party and second party key negotiation algorithms.

24. The method of claim 22, further comprising:

encrypting the electronic book using the shared transaction symmetric key;

delivering the encrypted electronic book to the second party; and

decrypting the encrypted electronic book using the shared transaction symmetric key.

25. The method of claim 2, further comprising:

supplying the encrypted electronic book using a first communications path; and

supplying the symmetric key using a second communications path.

26. The method of claim 2, further comprising supplying the encrypted electronic book and the symmetric key using a same communications path.

27. The method of claim 26, wherein the encrypted electronic book and the symmetric key are supplied simultaneously.

28. The method of claim 1, wherein the encryption key is generated by a first seed key generation algorithm and the decryption key is generated by a second seed key generation algorithm.

29. The method of claim 28, wherein the first and the second key generation algorithms generate a seed key.

30. The method of claim 29, further comprising:

using the seed key at a first party location to generate a first shared transaction symmetric key in a sequence of keys;

encrypting the electronic book using the first shared transaction symmetric key;

delivering the encrypted electronic book to a second party;

using the seed key at a second party location to generate a shared transaction symmetric key corresponding to the first shared transaction symmetric key generated at the first party location;

decrypting the encrypted electronic book using the shared transaction symmetric key; and

repeating the process to generate a second and subsequent shared transaction keys to encrypt and decrypt subsequent electronic books.

31. The method of claim 1, wherein the encryption key and the decryption key are asymmetric.

32. The method of claim 31, wherein the electronic book is encrypted using one of a Merkle-Hellman Knapsack technique, a RSA technique, a Pohlig-Hellman technique and a Schnorr Signatures technique.

33. The method of claim 31, wherein the encryption key is a public key and the decryption key is a private key.

34. The method of claim 31, wherein the encryption key is a private key and the decryption key is a public key.

35. The method of claim 1, further comprising providing the decryption key with the encrypted electronic book.

36. The method of claim 35, further comprising encrypting the decryption key.

37. The method of claim 1, further comprising using a first cryptographic algorithm with the encryption key to encrypt the electronic book.

38. The method of claim 37, wherein the first cryptographic algorithm is one of DES, PKZIP and BLOWFISH.

39. The method of claim 1, further comprising using a second cryptographic algorithm with the decryption key to decrypt the encrypted electronic book.

40. The method of claim 1, wherein encrypted electronic books are delivered to home systems individually.

41. The method of claim 1, further comprising:

providing multiple electronic books to a home system; and

supplying the decryption key upon request for a particular electronic book by the home system.

42. The method of claim 1, wherein the encrypted electronic book is broadcast to multiple home systems simultaneously.

43. The method of claim 42, wherein the encryption key is a transaction symmetric key.

44. The method of claim 43, further comprising:

encrypting the transaction symmetric key using a first public key corresponding to a first home system;

encrypting the transaction symmetric key using second and subsequent public keys corresponding to second and subsequent home systems, respectively;

delivering the first through the subsequent encrypted transaction symmetric keys to the multiple home systems;

decrypting the delivered first encrypted transaction symmetric key at the first home system using a first private key;

decrypting the second and subsequent encrypted transaction symmetric keys at one or more of corresponding ones of the multiple home systems using second and subsequent private keys, respectively; and

decrypting the delivered encrypted electronic book at one or more of the multiple home systems using the decrypted transaction symmetric key.

45. The method of claim 44, further comprising:

assigning one or more of the multiple home systems to one or more predefined groups;

generating a group symmetric key for each of the one or more groups of home systems; and

distributing the corresponding group symmetric key to each home system in the one or more groups of home systems.

46. The method of claim 1, wherein the encrypted electronic book is delivered to a home system, the home system comprising:

a library; and

a viewer.

47. The method of claim 46, wherein security processing is completed in the library.

48. The method of claim 46, wherein security processing in completed in the viewer.

49. The method of claim 46, further comprising completing security processing between the viewer and the library.

50. The method of claim 49, further comprising:

receiving the encrypted electronic book at the library;

decrypting the received electronic book;

storing the decrypted electronic book in a memory;

retrieving the stored electronic book;

encrypting the retrieved electronic book using a symmetric key;

encrypting the symmetric key using a library private key;

delivering the encrypted electronic book and the encrypted symmetric key to the viewer;

decrypting the encrypted symmetric key using a viewer public key; and

decrypting the encrypted electronic book using the decrypted symmetric key.

51. The method of claim 50, wherein the symmetric key is randomly generated.

52. The method of claim 50, wherein the symmetric key is generated by a key generator process.

53. The method of claim 50, wherein the symmetric key is previously defined, further comprising retrieving the previously-defined symmetric key.

54. The method of claim 1, further comprising performing integrity checking of the electronic book.

55. The method of claim 54, wherein the step of integrity checking, comprises:

calculating a first hashing value based on content of the electronic book and a hashing algorithm;

associating the first hashing value with the electronic book

calculating a second hashing value using the decrypted electronic book and the hashing algorithm;

comparing the first and the second hashing values; and

storing the decrypted electronic book when the first and the second hashing values match.

56. The method of claim 54, wherein a digital signature algorithm is used to identify the sending party.

57. The method of claim 1, further comprising verifying an identity of a party sending the electronic book.

58. The method of claim 57, wherein the verifying step, comprises:

delivering a password with the electronic book;

comparing the delivered password with a pre-defined password; and

storing the delivered electronic book when the delivered password and the pre-defined password match.

59. The method of claim 57, wherein the verifying step comprises decrypting the delivered electronic book using the decryption key.

60. The method of claim 57, wherein the verifying step comprises

sending a delivery notification message from a sending party to a receiving party receiving the electronic book

encrypting a randomly generated message;

returning the randomly generated message to the sending party sending the delivery notification message; and

decrypting the randomly generated message;

re-encrypting the randomly generated message; and

returning the re-encrypted randomly generated message to the receiving party with the encrypted electronic book.

61. The method of claim 57, wherein the verifying step comprises using an ISO standard X.509 one-way authentication protocol.

62. The method of claim 1, further comprising verifying an identity of a first party requesting the electronic book.

63. The method of claim 62, wherein the verifying step, comprises:

receiving an electronic book request from the first party;

generating an authentication string;

sending the authentication string to the first party; and

returning a response message, wherein the response message, comprises:

an identifier that identifies the requested electronic book,

a signed authentication string, wherein the signed authentication string is signed using a one-way hash function and wherein the signed authentication string is encrypted, and

a first party certification information.

64. The method of claim 1, further comprising:

creating a non-secure metadata header for the electronic book;

creating a secure metadata header for the electronic book, wherein the secure metadata header includes one or more of an electronic book identifier, the decryption key, a decryption algorithm, a number of copies of the electronic book that are allowed to be derived from an original electronic book file, distribution and fair use features and integrity checking information; and

packaging the non-secure and the secure headers with the electronic book to create an electronic book distribution file.

65. The method of claim 64, further comprising:

compressing the electronic book distribution file; and

sending the electronic book distribution file to a receiving party.

66. The method of claim 65, wherein the receiving party is an operations center of a television distribution system.

67. The method of claim 65, wherein the receiving party is an electronic book home system.

68. The method of claim 65, wherein the receiving party is a library.

69. The method of claim 65, wherein the receiving party is a kiosk.

70. The method of claim 65, wherein the electronic book distribution file is distributed by a publisher.

71. The method of claim 65, wherein the electronic book distribution file is distributed by an operations center.

72. The method of claim 65, wherein the electronic book distribution file is distributed by a library.

73. The method of claim 65, wherein the electronic book distribution file is distributed by an electronic book home system.

74. The method of claim 65, wherein the electronic book distribution file is distributed at a kiosk.

75. The method of claim 65, wherein the electronic book distribution file is delivered from a first viewer to a second viewer.

76. The method of claim 65, wherein the electronic book distribution file is distributed over an Internet using a secure socket layer protected communication link.

77. The method of claim 76, wherein the receiving party sends an electronic book request message to request the electronic book, the request message including an Internet Protocol address of the receiving party.

78. The method of claim 77, wherein the request message includes a login and password sequence.

79. The method of claim 77, further comprising:

sending a certificate to the receiving party, the certificate including information identifying a sending party and a sending party public key;

verifying the certificate by comparing the information included in the certificate to expected values for the information;

sending an algorithms supported message to the sending party;

returning a selected algorithm to the receiving party;

generating a transaction symmetric key;

encrypting the transaction symmetric key using the sending party public key and the selected algorithm;

sending the encrypted transaction symmetric key to the sending party;

decrypting the encrypted transaction symmetric key using a sending party private key; and

using the transaction symmetric key to encrypt and to decrypt a transaction between the sending party and the receiving party.

80. The method of claim 76, wherein a sending party sends an electronic book distribution message to the receiving party, the distribution message including Internet Protocol address of the sending party.

81. The method of claim 80, wherein the distribution message further comprises a login and password sequence.

82. The method of claim 81, further comprising:

sending a certificate to the sending party, the certificate including information identifying a sending party and a receiving party public key;

verifying the certificate by comparing the information included in the certificate to expected values for the information;

sending an algorithms supported message to the receiving party;

returning a selected algorithm to the sending party;

generating a transaction symmetric key;

encrypting the transaction symmetric key using the receiving party public key and the selected algorithm;

sending the encrypted transaction symmetric key to the receiving party;

decrypting the encrypted transaction symmetric key using a receiving party private key; and

using the transaction symmetric key to encrypt and to decrypt a transaction between the sending party and the receiving party.

83. The method of claim 1, wherein the electronic book is delivered to a receiving party by a sending party, the method further comprising verifying that the receiving party received the electronic book.

84. The method of claim 83, wherein the verifying step, comprises:

generating a reply message;

encrypting the reply message using a private key of the receiving party;

encrypting the encrypted reply message using a public key of the sending party;

sending the doubly encrypted reply message to the sending party; and

decrypting the doubly encrypted reply message using a private key of the sending party and a public key of the receiving party.

85. The method of claim 83, wherein the verifying step comprises using an ISO standard X.509 two-way authentication protocol framework.

86. The method of claim 1, wherein encryption key information is suppled between a sending party and a receiving party using a telecommunications network.

87. The method of claim 86, wherein the telecommunications network comprises one or more of a television delivery system, a wired telephone network, a wireless telephone

network, a personal communications network (PCS), an Internet, an intranet, a local area network, a radio communications network, and an optical fiber network.

88. The method of claim 1, wherein encryption key information is supplied between a sending party and a receiving party using a portable memory storage device.

89. The method of claim 88, wherein the portable memory storage device includes one or more of a PCMCIA card, a CD ROM, a memory stick, and a smart card.

90. The method of claim 89, wherein the encryption key includes a valid time period of use.

91. The method of claim 89, wherein the portable memory storage device is updated remotely using a telecommunications network.

92. The method of claim 1, further comprising:

receiving the encrypted electronic book at a receiving party; and

storing the electronic book in an encrypted format in a memory storage device.

93. The method of claim 92, wherein the encrypted storage is performed at a driver level, comprising:

encrypting the electronic book using a memory storage device driver level; and

storing the encrypted electronic book at the memory storage device.

94. The method of claim 93, wherein the electronic book is encrypted using a symmetric key.

95. The method of claim 92, wherein the encrypted storage is performed at a file level, further comprising:

encrypting the electronic book using a unique symmetric key;

storing the encrypted electronic book in the memory storage device; and

storing the symmetric key, wherein the symmetric key is stored in a memory location apart from a memory location for the electronic book.

96. The method of claim 92, further comprising:

computing a first hashing value, using a one-way hashing algorithm and the electronic book, prior to encrypting the electronic book and storing the encrypted electronic book in the memory storage device;

storing the first hashing value;

retrieving the encrypted electronic book and the first hashing value;

decrypting the retrieved encrypted electronic book;

computing a second hashing value using the retrieved decrypted electronic book and the one-way hashing algorithm; and

comparing the first and the second hashing values, wherein when the first and the second hashing values coincide, an integrity of the stored encrypted electronic book is assured.

97. An electronic book viewer for receiving an electronic book from a sending party, and for storing and displaying the electronic book, comprising:

a receiver that receives encrypted electronic books and encryption information;

a memory coupled to the receiver that stores the encrypted electronic books and the encryption information;

a processor coupled to the memory that processes the encryption information using an encryption/decryption algorithm, wherein the processor comprises:

a key generator that generates encryption and decryption keys; and

a transmitter coupled to the processor that sends encryption information to the sending party, wherein the encryption information includes information that allows encryption and decryption of the electronic book and encryption and decryption of encryption and decryption keys.

98. The electronic book viewer of claim 97, wherein the encryption keys and the decryption keys are symmetric keys.

99. The electronic book viewer of claim 98, wherein the symmetric keys are generated randomly.

100. The electronic book viewer of claim 98, wherein the memory stores the symmetric keys, and wherein the processor retrieves a stored symmetric key from the memory.

101. The electronic book viewer of claim 98, wherein the receiver receives a transaction symmetric key from a certificate authority, and the memory stores the transaction symmetric key.

102. The electronic book viewer of claim 101, wherein the processor generates a transaction symmetric key request, the transmitter sends the request to the certificate authority and the receiver receives an encrypted transaction symmetric key, and wherein the processor uses the encrypted transaction symmetric key to decrypt the encrypted received electronic book.

103. The electronic book viewer of claim 98, wherein the symmetric key is encrypted with a private key and a private encryption algorithm and wherein the processor decrypts the encrypted symmetric key using a public key and a public key decryption algorithm.

104. The electronic book viewer of claim 98, wherein the processor further comprises a shared key negotiation algorithm, wherein the symmetric key is a shared transaction symmetric key, and wherein the processor negotiates with the sending party to generate the shared transaction symmetric key.

105. The electronic book viewer of claim 97, wherein the processor further comprises a first seed key generation algorithm and a second seed key generation algorithm, the processor using the first seed key generation algorithm to generate an encryption key and using the second seed key generation algorithm to generate a decryption key.

106. The electronic book viewer of claim 97, wherein an encryption key is a public key and a decryption key is a private key.

107. The electronic book viewer of claim 97, wherein the encryption key is a private key and the decryption key is a public key.

108. The electronic book viewer of claim 97, wherein the receiver receives a decryption key with the electronic book.

109. The electronic book viewer of claim 108, wherein the decryption key is encrypted before shipment to the electronic book viewer.

110. The electronic book viewer of claim 97, wherein the electronic book is encrypted using one of DES, PKZIP and BLOWFISH encryption algorithms.

111. The electronic book viewer of claim 97, wherein the encrypted electronic books are broadcast to the electronic book viewer.

112. The electronic book viewer of claim 111, wherein the electronic book is encrypted using a first public key system corresponding to the electronic book viewer.

113. The electronic book viewer of claim 97, wherein the electronic book viewer is assigned to one or more predefined groups of electronic book viewers.

114. The electronic book viewer of claim 97, further comprising a library unit coupled to the electronic book viewer, wherein the library unit completes security processing.

115. The electronic book viewer of claim 97, wherein the processor includes an integrity checking algorithm.

116. The electronic book viewer of claim 97, wherein the processor includes a verification algorithm that verifies an identity of the sending party.

117. The electronic book of claim 97, wherein the processor includes an authentication algorithm.

118. The electronic book of claim 97, wherein the sending party is a book publisher.

119. The electronic book viewer of claim 97, wherein the sending party is an operations center of a cable television delivery system.

120. The electronic book viewer of claim 97, wherein the sending party sends electronic books using an Internet web site.

121. The electronic book viewer of claim 97, wherein the sending party is a kiosk.

122. The electronic book viewer of claim 97, wherein the sending party is another electronic book viewer.

123. The electronic book viewer of claim 97, wherein the electronic book viewer receives encrypted electronic books and encryption information using a telecommunications network.

124. The electronic book viewer of claim 123, wherein the telecommunications network includes one or more of a television delivery system, a wired telephone system, a wireless telephone network, a personal communications network, a wired Internet system, a wireless Internet system, an intranet, a local area network, a radio communications network, and an optical fiber network.

125. The electronic book viewer of claim 97, further comprising a data entry port, wherein the electronic book viewer receives encryption key information using the data entry port and a portable memory storage device.

126. The electronic book viewer of claim 125, wherein the portable memory storage device includes one or more of a PCMCIA card, a CD ROM, a smart card and a memory stick.

127. The electronic book viewer of claim 126, wherein the encryption key includes a valid time period of use.

128. The electronic book viewer of claim 126, wherein the encryption key includes a valid time period of use.

129. The electronic book viewer of claim 125, wherein the portable memory storage device is updated remotely using a telecommunications network.

130. A system for encrypting an electronic book for delivery from a first party to a second party, comprising:

a first interface that receives and transmits electronic books and encryption information;

a first memory coupled to the first interface that stores the electronic books and the encryption information;

a first processor coupled to the first interface and the first memory that processes the encryption information and encrypts and decrypts the electronic books;

a second interface that receives electronic books transmitted from the first party, and that receives and transmits encryption information;

a second memory coupled to the second interface that stores the received electronic books and the encryption information; and

a second processor coupled to the second interface and the second memory that processes the encryption information and that decrypts the received electronic books.

131. The system of claim 130, wherein the first and the second parties are coupled to a communications network, and wherein the encryption information and the electronic books are transmitted and received using the communications network.

132. The system of claim 131, wherein the communications network includes one or more of a television delivery system, a wired telephone system, a wireless telephone network, a personal communications network, a wired Internet system, a wireless Internet system, an intranet, a local area network, a radio communications network, and an optical fiber network.

133. The system of claim 130, wherein the encryption information includes an encryption key and a decryption key.

134. The system of claim 133, wherein the encryption key and the decryption keys comprise a symmetric key.

135. The system of claim 134, wherein the first processor comprises a first key generator, the first key generator generating the symmetric key.

136. The system of claim 135, wherein the first key generator generates the symmetric key randomly.

137. The system of claim 134, wherein the second processor comprises a second key generator, the second key generator generating the symmetric key.

138. The system of claim 137, wherein the second key generator generates the symmetric key randomly.

139. The system of claim 134, wherein the first processor and the second processor retrieve the symmetric key from the first and the second memories, respectively.

140. The system of claim 134, wherein the symmetric key is a transaction symmetric key, the transaction symmetric key supplied by a third party.

141. The system of claim 140, wherein the third party is a certificate authority.

142. The system of claim 141, wherein the certificate authority issues the transaction symmetric key encrypted.

143. The system of claim 142, wherein the transaction symmetric key is encrypted by the certificate authority using a first party symmetric key.

144. A method for secure distribution of electronic books, comprising:

receiving an electronic book;

obtaining an encryption key;

processing the electronic book using the encryption key and an encryption algorithm;

sending the encrypted electronic book to a recipient;

obtaining a decryption key; and

decrypting the encrypted electronic book using the decryption key and a decryption algorithm.

145. The method of claim 144, wherein the encrypted electronic book is broadcast to multiple home systems simultaneously.

146. The method of claim 145, wherein the encryption key is a transaction symmetric key.

147. The method of claim 146, further comprising:

encrypting the transaction symmetric key using a first public key corresponding to a first home system;

encrypting the transaction symmetric key using second and subsequent public keys corresponding to second and subsequent home systems, respectively;

delivering the first through the subsequent encrypted transaction symmetric keys to the multiple home systems;

decrypting the delivered first encrypted transaction symmetric key at the first home system using a first private key;

decrypting the second and subsequent encrypted transaction symmetric keys at one or more of corresponding ones of the multiple home systems using second and subsequent private keys, respectively; and

decrypting the delivered encrypted electronic book at one or more of the multiple home systems using the decrypted transaction symmetric key.

148. The method of claim 147, further comprising:

assigning one or more of the multiple home systems to one or more predefined groups;

generating a group symmetric key for each of the one or more groups of home systems; and

distributing the corresponding group symmetric key to each home system in the one or more groups of home systems.

149. The method of claim 144, further comprising storing the electronic book in memory as an encrypted file.

150. The method of claim 144, wherein the encrypted electronic book is sent by a publisher and the recipient is an operations center of an electronic book distribution system.

151. The method of claim 144, wherein the encrypted electronic book is sent by an operations center and the recipient is a home system.

152. The method of claim 144, wherein the encrypted electronic book is sent by a lending facility and the recipient is a home system.

153. The method of claim 144, wherein the encrypted electronic book is sent by a home system library and the recipient is a home system viewer.

154. The method of claim 144, wherein the encrypted electronic book is sent by a first home system viewer and the recipient is a second home system viewer.

155. The method of claim 144, further comprising creating a protected metadata header related to the electronic book, wherein the protected metadata header comprises an electronic book identifier, a metadata format identifier, the decryption key, and a decryption algorithm.

156. The method of claim 155, wherein the protected metadata header is provided with the encrypted electronic book.

157. The method of claim 155, wherein the protected metadata header is provided separate from the encrypted electronic book.

158. The method of claim 155, wherein the protected metadata header further comprises a number of allowed copies of the encrypted electronic book, distribution features supported for the electronic book, fair use features and integrity checking information.

159. The method of claim 158, wherein the fair use features comprise using the electronic book for a specified time.

160. The method of claim 159, wherein the fair use features comprise a print enable function.

161. The method of claim 160, wherein the print enable function enables a specified number of copies of the electronic book to be printed.

162. The method of claim 158, wherein the distribution features comprise a loan enable feature, the loan enable feature allowing a sending party to send the electronic book to one or more recipients.

163. The method of claim 144, further comprising compressing the encrypted electronic book before sending to the recipient.

164. The method of claim 144, further comprising authenticating an identity of the recipient.

165. The method of claim 164, wherein the authenticating step comprises using a digital signature algorithm.

166. The method of claim 164, wherein the authenticating step comprises using a password.

167. The method of claim 144, wherein the step of sending the encrypted electronic book comprises sending the encrypted electronic book to a remote location, wherein the recipient retrieves the encrypted electronic book from the remote location.

168. The method of claim 167, wherein the remote location is an Internet website.

169. The method of claim 167, wherein the remote location is a computer, and wherein the recipient is coupled to the computer.

170. The method of claim 169, wherein the recipient and the computer are coupled by a communications network.

171. The method of claim 169, wherein the communications network is an infra red network.

172. The method of claim 169, wherein the communications network is a radio frequency network.

173. The method of claim 167, wherein the sending party removes the encrypted electronic book from the remote location after a specified time.

174. The method of claim 144, wherein the recipient is a home system, further comprising:

registering the home system with the sending party;

assigning the home party an electronic book deposit location; and

sending electronic books for the home system to the deposit location.

175. The method of claim 174, further comprising sending decryption information to the deposit location.

176. The method of claim 174, wherein the sending party obtains information from the home system during the registering step, and wherein the information includes an internal serial number of the home system.

177. The method of claim 144, further comprising:

generating a reply message upon receipt of the encrypted electronic book; and

returning the reply message to the sending party, the reply message indicating receipt of the encrypted electronic book.

178. The method of claim 144, further comprising:

generating a reply message upon decrypting the encrypted electronic book; and

returning the reply message to the sending party.

179. The method of claim 144, wherein the recipient is a public viewer.

180. The method of claim 144, further comprising sending a data header with the encrypted electronic book, wherein the data header comprises a time duration for retention of the electronic book by the recipient.

181. The method of claim 144, wherein a first part of the electronic book is encrypted and a second part of the electronic book is not encrypted.

182. The method of claim 144, further comprising applying a copyright notice to the electronic book.

183. The method of claim 144, wherein stenographic information is embedded in the electronic book.

184. The method of claim 183, wherein the stenographic information identifies a valid recipient viewer.

185. The method of claim 184, wherein a viewer displays only electronic books for which the stenographic information matches the displaying viewer.

186. The method of claim 144, wherein the encryption and the decryption algorithms are updated using a software download over a distribution network.

187. The method of claim 144, wherein the encryption and the decryption algorithms are updated using physical media.

188. The method of claim 187, wherein the physical media comprises one of a PCMCIA card, a smart card, a memory stick and a memory device.

189. The method of claim 144, wherein the electronic book comprises one or more pages and wherein a viewer decrypts the electronic book page by page, each page of the one or more pages of the electronic book being decrypted just before viewing.